QBE Global Shared Services Centre

Philippines

GSSC Privacy Policy

DOCUMENT CONTROL

Reference No.	GSSC-P-2018-00-JUN-001
Name	GSSC Privacy Policy
Category	Data Privacy
Document Owner	GSSC Governance, Risk and Compliance
Document Classification	Policy / For Internal Use Only
Frequency of review	Every Three Years
Date Created	June 2018
Date Last Revised	New Policy
Reviewed by	Elmer Mendoza, GSSC Chief Risk Officer
	Fritz Dumol, GSSC Compliance Officer
	GSSC Senior Leadership Team
Approved by	Mark Woolfrey, GSSC Executive General Manager
Approval Date	18 June 2018
Effective Date	16 July 2018
Status:	Final v.1.1
Point of contact:	Rome Gamboa, Risk Manager, Governance Risk & Compliance (GRC) rome.gamboa@qbe.com

DOCUMENT REVISION HISTORY

Version	Date	Updated By	Description
Draft v.1.1	30 May	Rome Gamboa	Presented to Senior Leadership Team (RMF)
Draft v.1.1	5 June 2018	Rome Gamboa	Added a few sections in Appendix 3 - Definitions and Acronyms
Final v.1.	8 June 2018	Rome Gamboa	Circulated document for review
Final v.1.	13 June 2018	Rome Gamboa	Approval from EGM
Final v.1.1	24 Aug 2018	Rome Gamboa	Defined composition of QBE GSSC
			Added intention of the Policy
			Updated Scope wording
Final v.1.2	28 Nov 2018	Rome Gamboa	Added section prohibiting the use of personal data in developing and maintaining reference materials
Final v.1.3	18 Jan 2019	Rome Gamboa	Added the email address of the DPO/ DPT

Table of Contents

I. INTRODUCTION

The QBE Group Shared Services Centre (QBE GSSC) is committed to respecting the privacy and protecting the personal information of our customers and employees from misuse or unauthorized disclosure and in complying with privacy laws.

The Philippines' first comprehensive data protection law, the Data Privacy Act of 2012 took effect on 8 September 2012 and the Implementing Rules and Regulations (IRR) were issued on 2016 and became enforceable on 9 September 2016. The Act is a legislation that focuses on the protection of fundamental human right of privacy and the obligations of companies who act as Personal Information Controller (PIC) and/or Personal Information Processor (PIP). Non-compliance of companies to this Act may result to stiff penalties of imprisonment of not more seven (7) years and a fine of up to Php5-M.

QBE GSSC values its reputation and aims to maintain high ethical standards in the conduct of its business affairs. The actions and conduct of employees as well as others acting on QBE's behalf, such as agents and third parties, are key to maintaining these standards.

Failure to ensure adequate privacy compliance exposes QBE to the risk of breaching privacy laws, and may result in significant fines and penalties, reputational damage and other adverse regulatory impacts, additional costs and third party claim damages.

This document sets out the Policy Guidelines for the QBE Group Shared Services Centre ("**QBE GSSC**" or "**GSSC**"), which includes the following entities:

- QBE Group Shared Services Limited – Philippine Branch ("**QGSSL**")[1]
- QBE Management Services (Philippines) Pty Ltd., otherwise known as "QBE Management Services Asia Operating Headquarters" ("**QBE ROHQ**").

This GSSC Data Privacy Policy (hereafter, the "Policy") is intended as a guideline to the Group Policy in order to manage compliance with local regulatory requirements.

II. PURPOSE

This Privacy Policy establishes minimum standards for QBE GSSC's approach to comply with privacy requirements. It sets out the principles essential for managing compliance with privacy laws of the jurisdictions in which QBE operates.

Approval and application

This Policy reflects the principles of the Group Privacy Policy and applies to all employees and contractors, of QBE GSSC. This manual shall also be endorsed by the Data Protection Officer (DPO) to the GSSC Senior Leadership (SLT) team for their approval.

III. SCOPE

Scope

All personnel working for/with QBE GSSC, which includes all management, employees, contractors and consultants are subject to the QBE GSSC Privacy Policy. It covers all personal information collected or processed by or on behalf of QBE GSSC including its Personal Information Processor/s (PIP/s).

This Policy covers the treatment of personal information gathered and used by QBE GSSC for lawful business purposes. This Policy also covers the personal information shared with authorized third parties or that third parties shared with QBE GSSC.

Any requests for exceptions to this policy should firstly be referred to GSSC's designated Data Privacy Officer (DPO). Written approval from the DPO should then be forwarded to the person requesting the exception.

Applicable Privacy Law
The Philippine Data Privacy Act of 2012 (DPA) is a law to address crimes and concerns related to data privacy. It (1) protects the privacy of individuals while ensuring the free flow of information to promote innovation and growth; (2) regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure and destruction of personal data; and (3) ensures that the Philippines complies with international standards set for data protection. The National Privacy Commission (NPC) is the Philippine regulatory body that will promulgate and enforce the DP Act of 2012.
GSSC processes information based on the regulatory requirements of processes offshored to the GSSC and has an obligation to notify their respective designated compliance, privacy officer, or equivalent, in the event of a privacy breach.

IV. APPROACH

This section sets out the key principles and requirements that govern QBE GSSC's approach to managing compliance with privacy laws.

Principles
The following principles govern QBE GSSC's approach to managing compliance with privacy laws.

The types of personal information QBE GSSC collect from the data subjects, and how QBE GSSC use and disclose this personal information shall be allowed subject to the adherence to the principles of transparency, legitimate purpose, and proportionality.

1. Transparency
   The Data Subject must be aware of the nature, purpose, and extent of the Processing of his or her Personal Data by the Company, including the risks and safeguards involved, the identity of persons and entities involved in processing his or her Personal Data, his or her rights as a Data Subject, and how these can be exercised. Any information and communication relating to the Processing of Personal Data should be easy to access and understand, using clear and plain language.

2. Legitimate Purpose
   The Processing of Personal Data by the Company shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

3. Proportionality
   The Processing of Personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal Data shall be processed by the Company only if the purpose of the Processing could not reasonably be fulfilled by other means.

Collection
1. QBE GSSC will collect personal information that is reasonably necessary to offer, issue, administer and manage the services QBE GSSC offer and will not collect more than is necessary for these purposes.
2. QBE GSSC data subjects will be informed of the purpose for which QBE GSSC will use their data at the time QBE GSSC collects it or, where this is not possible, as soon as practicable thereafter.

Type of information collected

1. Collection of Personal Information

   QBE GSSC must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the QBE GSSC's functions or activities. QBE GSSC may collect personal information only by lawful and fair means and not in an unreasonably intrusive way. Whenever employees and contractors collect personal information about an individual, they must take reasonable steps to ensure that the individual is aware of the following:

   a The identity and contact details of QBE GSSC as the organization collecting and storing the information;
   b The fact that data subject is able to gain access to the information and seek correction;
   c The purposes for which the information is collected;
   d The intended recipients or organizations to which QBE GSSC usually discloses information of that kind, including any overseas recipients and the countries in which those recipients are likely to be located;
   e The fact that data subject may make a privacy complaint and how QBE GSSC will deal with it;
   f Any law that requires the particular information to be collected;
   g The main consequences (if any) for the individual if all or part of the information is not provided; and
   h The period of retention of information after processing.

   Where it is reasonable and practical to do so, QBE GSSC will collect personal information about an individual only from that individual. If however this information is collected from someone else, employees and contractors must act reasonably to ensure the individual is or has been made aware of the matters listed above.

2. Collection of Sensitive Personal Information

   Sensitive Personal Information is information or an opinion:

   a About an individual's race, ethnic origin, marital status, age, colour, and religious, philosophical or political affiliations;
   b About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings or the sentence of any court in such proceedings;
   c Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
   d Specifically established by an executive order or an act of Congress to be kept classified.

   Employees and contractors must only collect sensitive information:

   a Where the information is reasonably necessary for one or more of the Group's functions or activities and with the individual's consent; or
   b If the collection is required by law.

How information is collected

1. Subject to regulatory requirements, QBE GSSC may collect information directly from the data subjects.
2. If QBE GSSC is permitted by law to do so, QBE GSSC may also collect or purchase information from third parties.

3. Upon request and where required by regulatory requirements, QBE GSSC will take reasonable steps to let the data subjects know how we have sourced their personal information and to inform them of the purposes for which we will use their personal information.
4. QBE GSSC collects information about data subjects and their interactions with us, for example when the data subject, phone us or visit any of our websites. When they use our website or mobile applications they agree that we may collect information about their location or activity including IP address, telephone number and whether they have accessed third party sites and that we may collect this information using cookie technology.

Receiving Unsolicited Personal Information

Where employees and contractors receive unsolicited personal information about an individual they must determine (within a reasonable time) whether they could have collected the information in accordance with section 2.1.1 above. If so, then this policy shall apply to the processing of such information. If not, then they must as soon as practical (but only if lawful and reasonable) either destroy or de-identify the information.

Collection of Personal information for Research

QBE GSSC may also collect personal information for research about an individual from a party other than the individual concerned if:

1. The personal data is publicly available;
2. The consent of the data subject for purpose of research;
3. Adequate safeguards are in place;
4. No decision directly affecting the data subject shall be made on the basis of the data collected or processed.

Collection of Personal information for Mobile Application

1. QBE's mobile application that does any of the following should have a Privacy Notice:
    a Collects personal data (e.g., guests filling in QBE GSSC's web forms, feedback forms, applications for employment, shopping online, posting of product reviews, and so on),
    b Uses cookies and/or QBE GSSC web beacons,
    c Covertly collects personal data (e.g., IP addresses, e-mail addresses, and so on), and
    d Requests mobile device permissions (e.g., camera, microphone, contacts, phone, and so on)
2. Mobile applications, if performing any of the items mentioned (a) above, cannot continue to do so without obtaining the mobile application user's prior permission and providing the user with access to information about and where the data will be used. Comply with the sections IV. APPROACH, Type of information collected, 1. Collection of Personal Information, 2. Collection of Sensitive Personal Information, How information is collected, and Consent.
3. The Privacy Notice should disclose the personal data collected, including the use of cookies and/or QBE GSSC web beacons and the mobile device permissions accessed by the mobile application. Comply with the provisions in 2.1.3 How information is collected. Establish a cookie policy when needed.
4. Available on the profile page of the mobile application so mobile application users are able to read about the Privacy Notice before downloading the app.
5. Available within the mobile application, either with a direct link to a URL from the QBE GSSC website or embedded in the mobile application. Users must be able to easily find and read any legal agreements they are subject to.

Access to and Correction of Personal Information

1. As a general rule, QBE GSSC will, on request by an individual, provide them with access to their personal information within a reasonable time after such request is made and will consider a request from the individual for correction of that information.
2. The DPO cannot impose unreasonable charge upon the individual to cover the cost of locating, retrieving, reviewing and copying any material requested by the individual.

3. The DPO may however choose not to provide an individual with access to such information. This would include cases where:
    a. QBE GSSC reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
    b. Providing access would have an unreasonable impact on the privacy and affairs of other individuals;
    c. The request for access is frivolous or vexatious or the information requested is trivial;
    d. The information relates to anticipated or existing legal proceedings and would not be discoverable in those proceedings;
    e. Providing access would reveal the intentions of QBE GSSC in relation to negotiations with the individual in such a way as to prejudice those negotiations;
    f. Providing access would be unlawful;
    g. Denying access is authorized under law or a court/tribunal order;
    h. Providing access would be likely to prejudice an investigation of possible unlawful activity or security, defense or international relations; or
    i. Providing access would be likely to prejudice activities which are carried out by QBE GSSC on behalf of an enforcement body; or
    Where an individual:
        i Has been refused access to their personal information which QBE GSSC holds about them;
        ii Having requested correction of their personal information, is refused.

    Then in such cases the QBE GSSC will give the individual a written notice that sets out:
        i The reasons for the refusal where it is reasonable to do so; and
        ii The way in which the individual may make a complaint about such refusal.

Consent

1. Where required under regulatory requirements, QBE GSSC will obtain customer consent to collect, use and disclose personal information at the time the customer first engages with us, or as soon as practicable thereafter.
2. Subject to regulatory requirements, data subject may modify or withdraw their consent, or opt-out of receiving direct marketing at any time.
3. In light of our obligations under applicable privacy law, QBE GSSC must ensure that appropriate wording is included in their consent form where QBE GSSC will receive, or have access to any personal information from its clients and employees.

Use and disclosure

1. QBE GSSC will only use and disclose personal information and sensitive personal information for the purpose for which it was collected, for related purposes (or where permitted), for any other purpose allowed by law.
2. QBE GSSC will maintain the confidentiality of the data subjects' information unless disclosure is within the purposes communicated to the data subject or with a data subject's consent or compelled under any law.
3. With the data subject's consent, QBE GSSC may use or disclose personal information for additional purposes from time to time, such as sharing claims information with other insurers and intermediaries
4. QBE GSSC may use, disclose or analyze personal information for the purpose of providing personalized products to our customers and for other internal analytics and research (e.g. fraud intelligence and investigation).

Use and disclosure of Government Related Identifiers

QBE GSSC employees and contractors must not use and/or disclose government related identifiers unless such use or disclosure is reasonably necessary for QBE GSSC to verify the identity of the individual for the purpose of QBE 's activities, or alternatively, the use or disclosure is required or authorized under law.

Direct marketing

1. Use of personal information for direct marketing purposes is permitted where:
    a. The information has been collected from the individual and the individual would reasonably expect QBE GSSC to use it for that purpose; or
    b. The information has been collected from someone other than the individual and QBE GSSC has either obtained the individual's consent, or it is impractical for QBE GSSC to obtain the individual's consent before that particular use
2. Use of sensitive personal information for direct marketing is permitted only when the individual has consented to the use or disclosure of the information for that purpose.
3. When contacting individuals for direct marketing in whatever form, the following conditions must be present:
    a. QBE GSSC provides a simple means by which the individual may easily request not to receive direct marketing communications from QBE GSSC;
    b. In each direct marketing communication with the individual, QBE GSSC draws to the individual's attention, or prominently displays a notice, that he or she may express a wish to "unsubscribe" or not to receive any further direct marketing communications;
    c. The individual has not made a request to QBE GSSC not to receive direct marketing communications; and
    d. QBE GSSC will not charge the individual for giving effect to a request not to receive direct marketing communications.

Third party and cross border disclosures

Subject to informing customers and, where required, obtaining their consent:

1. QBE GSSC may disclose personal information of data subject to other QBE Controlled Entities and third party service providers which may be located in other countries to assist us in providing relevant services and products to our customers.
2. QBE GSSC will take reasonable steps to ensure that appropriate arrangements are in place with third parties including ensuring that there is a formal written agreement in place that includes provisions covering the appropriate transfer and processing of the personal information by the third party. Please also refer to local policies and procedures and seek assistance the Data Protection Officer.
3. QBE GSSC may disclose personal information to any local or foreign government, law enforcement, dispute resolution, statutory or regulatory body as required by and in accordance with any law or regulation. Appropriate guidance and advice should be obtained from the Data Protection Officer before such disclosures are made.

Maintaining Data Quality

Employees and contractors must take reasonable steps to make sure that the personal information they collect, use or disclose is accurate, complete, up to date and not misleading.

Holding and storing customer personal information

1. Information of Data Subject may be held in physical format, as electronic data, in our software, systems or databases.
2. Data subject information may be stored in the cloud within or outside the country where the information was collected. Where information is stored in this way, QBE GSSC will take reasonable steps to ensure that appropriate arrangements are in place with third party cloud providers including ensuring that there is a formal written agreement. This agreement will include provisions covering the transfer and processing of the personal information by the third party and prevent them from using or disclosing personal information for any other purposes, require them to comply with applicable data protection/privacy laws and include obligations to take appropriate technical and organisational measures to safeguard the personal information.

Protecting personal information

1. Employees and contractors must take reasonable steps to protect the personal information QBE GSSC holds from misuse, interference and loss and from unauthorized access, modification or disclosure by implementing physical, technical and administrative security standards to secure and protect personal information in accordance with the QBE Information Security Policy and applicable regulatory requirements.
2. Employees and contractors must not keep personal information for longer than is necessary and must take reasonable steps to securely destroy or permanently de-identify personal information if it is no longer needed following the standards set by QBE GSSC.
3. It is strictly prohibited to use personal data in developing and maintaining reference materials such as, but not limited to Desktop Procedures (DTP), training materials, samples or artefacts (unless for lawful purposes, such as for investigation).

Destruction of personal information

QBE is subject to legal requirements to retain information for particular timeframes. Subject to local regulatory requirements, when QBE GSSC is no longer legally required to retain personal information, and QBE GSSC no longer need personal information for its collected purpose, QBE GSSC will take reasonable steps to destroy or de-identify it (to the extent possible). Employees should refer to QBE Information Security Policy for applicable retention periods.

Rights of the Data Subject

1. QBE GSSC will take reasonable steps to ensure the personal information that QBE GSSC collect, hold and disclose is accurate, up to date and complete. Data subjects can contact us to update personal information or advise us if the personal information QBE GSSC holds is not accurate, up to date or complete.
2. In addition to rights to have their personal information corrected, Data subjects also have legal rights in respect of how QBE GSSC use their personal data as provided under the Data Privacy Act of 2012 requirements. These may include rights to obtain a copy of their personal information and for information on how it is being used (subject access requests), rights to have their data deleted, rights to withdraw their consent for data being used for particular purposes (e.g. direct marketing or profiling) and rights to transfer their personal information to a third party. QBE GSSC will take reasonable steps to ensure compliance with these requirements.
3. For any concerns, you may forward this to qbegsscspo1@qbe.com.

Requirements

In order to comply with the QBE GSSC Privacy Policy, the following are required:

1. A risk assessment of the QBE GSSC's exposure to privacy laws.
2. Within three months of the effective date of this Policy, adoption of this QBE GSSC Privacy Policy that reflects the principles and requirements of the Group Privacy Policy.
3. A gap analysis has been completed by the QBE GSSC Governance, Risk and Compliance Department for DPO review to evidence that relevant sections of the Group Privacy Policy have been adopted locally.
4. Unless required by local legislative requirements, closure of any material gaps between the Group Privacy Policy and any existing Divisional Privacy Policy within twelve months from the effective date of this Group Privacy Policy.
5. QBE GSSC Privacy Guidelines that support this QBE GSSC Privacy Policy and provide more detailed information to:
    a. Enable, where appropriate, the development of QBE GSSC Policies, Guidelines and/or Procedures to manage local regulatory requirements; and
    b. Support the development of divisional compliance programs
6. QBE GSSC compliance programs, reflecting the requirements of the Group or local Policies and Group Guidelines and incorporating:

a. Local regulatory requirements;
b. Systems and controls to identify and manage privacy risks, including appropriate due diligence; confidentiality requirements on our employees and other representatives, as well as third parties; policies on document storage security; security measures for access to our systems; only providing employee access to information once proper identification or authentication has been undertaken (which may be by role specific access); controlling access to our premises; and website protection security measures.
c. A training and communications program;
d. An evaluation and monitoring process; and
e. A Divisional l issue, incident and breach reporting process.

7. From a Group-level, a Privacy Working Group providing advice, oversight, monitoring and quality assurance information.
8. From a Divisional-level, a Data Protection Team providing advice, oversight, monitoring and quality assurance information.

Data Incident Notification Protocols

1. Data incident notification protocols are established and maintained in order to deal with an incident (i.e. an inadvertent disclosure of data, lost or stolen data or improper movement of data across national borders) concerning any confidential QBE GSSC data, personal information or client data.
2. Employees and contractors must immediately notify the QBE GSSC DPO, with email address qbegsscspo1@qbe.com, within 24 hours if they become aware of a data incident to enable the appropriate assessment, investigation and remediation measures to be undertaken in a timely manner (including possible notification to local Privacy regulators and other relevant bodies).If the incident occurs or is discovered outside normal working hours this should be done as soon as practicable.
3. The DPO shall notify the Commission within seventy-two (72) hours upon discovery or a reasonable belief that a personal data breach has occurred. If and only if, the following are present:

    a. There is a breach of sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud;
    b. The data is reasonably believed to have been acquired by an unauthorized person; and
    c. Either the personal information controller or the NPC believes that the data breach is likely to give rise to a real risk of serious harm to the affected data subject.
4. If there is doubt as to whether notification is indeed necessary, consider:

    a. The likelihood of harm or negative consequences on the affected data subjects;
    b. How notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred; and
    c. If the data involves:
        i. Information that would likely affect national security, public safety, public order, or public health;
        ii. At least one hundred (100) individuals; and/or
        iii. Information required by all applicable laws or rules to be confidential; or Personal data of vulnerable groups
5. All events must be recorded in the Incident Management System. Initial investigation should be performed as soon as possible within 24 hours from the time the personal data breach was reasonably believed to have occurred. Delay may be allowed if the scope of the breach cannot be determined within the 24-hour period. However, the 72-hour period notification to the Commission must be religiously observed.
6. After notifying NPC, steps shall be taken to notify the affected data subject. Person designated by the PIC shall notify the data subjects individually through a secure means of communication either through written or electronic mail.
7. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects

Privacy Impact Assessment
Privacy Impact Assessment (PIA) should be completed when there are events that significantly change in the privacy environment, the significant events are as follows:

1. New or modification to the current process
2. New projects
3. Marketing initiatives
4. Changes in the IT System Infrastructure

For changes in the IT System Infrastructure, at minimum, the following triggers should be considered:

PIA Trigger	Description
Digitization of records	Converting paper-based records to electronic systems.
Anonymous to Non-Anonymous	Operations performed on existing personal information database changes anonymous information into Sensitive Personal Information (SPI) or Personally Identifiable Information (PII).
Significant System Management Changes	New uses of existing IT systems, including application of new technologies, significantly changes how SPI or PII is managed in the system. For example, when the company employs new relational database technologies or web-based processing to access multiple data stores, such additions could create a more open environment and avenues for exposure of data that previously did not exist.
Significant Merging	The company adopts or alters business processes so that databases holding PII are merged, centralized, matched with other databases or otherwise significantly manipulated. For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create privacy concerns not previously an issue.
New User Access Mechanism	User-authentication technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by users (including Third Party users).
External Sources	The company systematically incorporates into existing information systems, databases of personally identifiable information purchased or obtained from third parties or public sources. An exception to this trigger would be merely querying such a source on an ad hoc basis using existing technology.

V. RESPONSIBILITIES

Objective: This section sets out the responsibilities and requirements under this Group Privacy Policy, with further information provided in the Group Privacy Guidelines.

GSSC Senior Leadership Team (SLT)

1. The SLT is responsible for review and, if thought appropriate, approval of this Policy, and oversight of breaches reported by the Data Protection Team (DPT).

2. The SLT is responsible for adoption of an equivalent divisional or localized Privacy Policy within three months of this Policy's effective date; and oversight of its operation by Divisional management.

GSSC Executive General Manager (EGM)

1. The GSSC EGM is responsible for ensuring requirements found on section IV. APPROACH, Requirements are in place. The EGM may require prior validation from the Data Privacy Team (DPT) or from any other appropriate GSSC department to ensure that necessary actions are taken and implemented

Governance Risk & Compliance (GRC)

1. GRC owns this Privacy Policy and is responsible for reporting breaches to the regulator, National Privacy commission (NPC).
2. GRC is responsible for establishing and managing compliance controls and for monitoring and oversight of privacy compliance.

Data Protection Officer

Implementing practices, procedures and systems relating to the GSSC's functions or activities that:

1. Will ensure the QBE GSSC complies with applicable privacy laws and privacy principles; and
2. Will enable the QBE GSSC to deal with enquiries or complaints from individuals about the QBE GSSC's compliance with applicable privacy laws and privacy principles.
3. Considering requests from individuals for access to, and correction of, personal information
4. Receiving complaints from an individual regarding an alleged breach of privacy by QBE GSSC.
5. Investigating and resolving complaints internally through mediation with the individual.

Employees

Employees are responsible for understanding and complying with the applicable Group or Divisional Policies, Guidelines and/or Procedures and applicable privacy law requirements.

Employees are also responsible for:

1. Attending and participating in relevant training sessions;
2. Reporting breaches of Privacy Policies or privacy laws to the Data Protection Team (or using the process set out in the appropriate Whistleblowing Policy); and
3. Seeking assistance from Data Protection Team where privacy issues arise.

Data Protection Team (DPT)

1. The Data Protection Team is responsible for providing advice, oversight, monitoring, quality assurance and evaluation of QBE GSSC's approach to privacy compliance.

VI. COMPLIANCE MONITORING AND REPORTING

1. Non-compliance with this policy may result in a breach of the QBE GSSC Privacy Policy, the Data Privacy Act of 2012 and other applicable laws.
2. QBE GSSC shall maintain the inventories of Personal Information Processing systems. Significant changes in the Personal Information Processing Systems shall be updated to the NPC within two (2) months after the implementation of the change.
3. QBE GSSC shall renew its annual registration to the National Privacy Commission within two (2) months prior to the deadline of 8th of March of the year

Consequences of non-compliance

1. For QBE GSSC and its employees, non-compliance with this Policy could have serious consequences, including fines and reputational damage.
2. For employees, non-compliance with privacy requirements could lead to disciplinary action initiated by QBE, including dismissal.

VII. EDUCATION AND AWARENESS

QBE GSSC employees must have access to all applicable Data Privacy policies, procedures, guidelines, incident reporting and Privacy Impact Assessment. Classroom training or E-learning must be developed for this purpose. Prospectively, subsequent communication of any changes will also be released /communicated via training materials.

Training materials include the following:

a. Salient features of the DP IRR;
b. Local Policies/Guidelines on Data Privacy;
c. Roles and Responsibilities of Heads of Business Units/Employees
d. Data Privacy Incident Reporting;
e. Breach Reporting
f. Privacy Impact Assessment;
g. Violations to the policy

VIII. EXCEPTIONS

Any requests for exceptions to this policy should firstly be referred to the DPO. Written approval from the DPO should then be forwarded to the person requesting the exception.

IX. AMENDMENTS

This policy will be reviewed at least every 3 years from its issue date or earlier if deemed required by the DPO. All policy changes should be drafted by the DPO and approved by the QBE GSSC Senior Leadership Team.

Appendix 1 – Suggested wording for QBE GSSC contract

A. Company shares data to the Third Party

"You agree to comply with to the Data Privacy Act of 2012 (DPA) with respect to any personal information (as that term is defined in the DPA) which you obtain in connection with provision of the services under this agreement. In particular, you agree that in performing the services you will not collect, use, store, and disclose any personal information except to the extent necessary for the purposes of this agreement. Further, you agree to implement appropriate security, technical and organizational measures as mandated in the Act, and to delete or return all personal information after the end of the provision of services related to this agreement, or at the instruction from QBE GSSC DPO."

B. Company obtains personal data from the Third Party

"We will Process the Personal Data in accordance with applicable law and professional regulations including (without limitation) the Data Privacy Act of 2012. We will require any service provider that Processes Personal Data on our behalf to adhere to such requirements. You warrant that you have the authority to provide the Personal Data to us in connection with the performance of the Services and that the Personal Data provided to us has been processed in accordance with applicable law."

Appendix 2 – Suggested wording for an QBE GSSC Consent Form- (for Half Pager Forms)

"To the extent necessary to provide the services to you and to your employer, you hereby authorize QBE GSSC to (1) obtain personal information from you, or from your employer, and (2) retain adequate documentation of the file in line with applicable laws and professional standards 10 years after the termination of the Services."

Appendix 3 - Definitions and Acronyms

For the purpose of this Policy, the following definitions and acronyms apply.

Term	Definition
Access	Access refers to an individual's right to see and know about his or her own personal information that an organization holds.
Collection	An organization collects personal information if it gathers, acquires or obtains information from any source, by any means, in circumstances where the individual is identified or is reasonably identifiable. It includes information that: • is publicly available information about an identifiable individual that an organization comes across; • information the organization receives directly from the individual; and • information about an individual an organization receives from somebody else.

Controlled Entity	As defined in Australian Accounting Standard AASB 10. Each controlled entity is deemed to be part of a Division. Controlled entities include all (re)insurance companies, agencies and service companies. Note: a Controlled Entity may be defined differently or more broadly depending on Division.
Cookie	A cookie is a piece of information in a small text file that is stored in an internet browser or elsewhere on a hard drive.
Data Subject	Refers to an individual whose personal information is processed.
Data Protection Officer (DPO)	Refers to an individual accountable for ensuring the compliance by the PIC or PIP with the DPA, its IRR, issuances by the NPC, and other applicable laws and regulations relating to privacy and data protection.
Data Protection team (DPT)	The functional group composed of the DPO, Deputy DPO & Compliance Officer who are responsible for providing advice, oversight, monitoring, quality assurance and evaluation of QBE GSSC's approach to privacy compliance.
Direct Marketing	Direct marketing includes activities that promote the sale or purchase of products or services or promote charitable fundraising where the individual is approached directly. It includes in-person approaches to people's houses and approaches by mail, e-mail, facsimile and phone. It includes individually targeted approaches by these means where people are encouraged to buy services at a distance (for example to buy by phone, mail or website) or to visit retail and service outlets or to donate to a cause by one of these means.
Division	Division One of QBE Group's operating divisions, including: • Australian and New Zealand Operations (ANZO); • Emerging Markets (EM); • European Operations (EO); • Group Shared Services Centre (GSSC); • North American Operations (NA); • Equator Reinsurances Limited; and • Group Head Office (GHO). References to Division also apply to Regions forming part of that Division.
GGC	Group General Counsel

Personal Information	Refers to any information, whether recorded in a material form or not, from which the identity of an individual Is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
Primary Purpose	The primary purpose is the dominant or fundamental reason for information being collected in a particular transaction. There can only be one primary purpose of collection for a particular transaction. When an individual gives (and an organization collects) personal information, the individual and the organization almost always do so for a particular purpose, for example, to buy or sell a particular product or to receive a service. This is the primary purpose of collection, even if the organization has some additional purposes in mind. These additional purposes will always be secondary purposes for that transaction, even if the organization tells the person about them, and even if the organization obtains the individual's consent to use or disclose the information for those additional purposes.
Privacy Working Group	A QBE internal group consisting of representatives from Group, and Divisional Compliance Departments.
QBE	QBE Insurance Group Limited and its Controlled Entities
Reasonable	Generally speaking, they relate to decisions or steps to be taken by organizations in particular circumstances (for example, when collecting, correcting or using and disclosing information) or to expectations of individuals in those circumstances. Determining what is reasonable involves considering the factual circumstances in which a person or organization is acting rather than the individual's or organization's view of what is reasonable or unreasonable.
Related Purpose	A related purpose includes all the purposes that are directly related purposes as well as certain additional ones. Related purposes must have some connection to, and arise in the context of, the primary purpose. Uses or disclosures for a related purpose would include uses or disclosures: • giving a person information closely associated with a particular product or service a person receives from an organization; or • notifying a person who has received a service or product from an organization in the past of a business change of address.

Required by Law	Required by law refers to circumstances where a law (other than the Data Privacy Act of 2012) requires an organization to collect, use or disclose or deny access to, personal information. In certain instances, failing to comply with such a legal requirement may be an offence. Such a law may specifically require an organization to collect, use, disclose or deny access. It may also be a law that gives another body, such as a government agency, a general information gathering power that includes the power to require an organization to disclose information to it.
Sensitive Personal Information	Sensitive personal information refers to personal information: • about an individual's race, ethnic origin, marital status, age, color and religious, philosophical or political affiliations; • About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of nay court in such proceedings; • Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or it denials, suspension or revocation and tax returns; and • Specifically established by an executive order or an act of Congress to be kept classified.
SLT	Senior Leadership Team
Third parties	May include information collected from customers, their employees and third parties on an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, criminal convictions, medical or health information membership of professional or trade associations and sexual life or preferences.
Use	Use of personal information relates to the handling of the personal information within the organization. Examples of uses of information are: • adding information to a database; • forming an opinion based on information collected and noting it on a file; and • including information in a publication.